

Important Contact Information

CA State Information Security Office (SISO) provides statewide direction and leadership in managing information security and risk management for the State's information assets, through policy and procedures, and promoting prevention, effective incident management, education, and compliance monitoring.

(916) 445-5239 - www.infosecurity.ca.gov/

CA Highway Patrol (CHP) provides intake and notification support for initial calls from state agencies as it relates to information security incidents. They have primary responsibility for investigations involving any type of crime against state assets, including computer crimes.

(916) 657-8287 - www.chp.ca.gov/

CA Office of Privacy Protection (COPP) advises government and private sector entities on policies and practices to protect confidential information regardless of media type. The COPP website offers links to a variety of privacy topics including recommended practices for privacy notification procedures and links to specific state privacy legislation.

(916) 574-8180 - www.privacy.ca.gov/

CA Office of HIPAA Implementation (CalOHI) directs and tracks additional incident reporting requirements for HIPAA-impacted agencies.

916) 654-3454 - www.calohi.ca.gov/



Incident Notification and Reporting

The State Administrative Manual (SAM) Section 4845 requires state agencies to notify and report information security incidents immediately upon discovery. Typically, it is the responsibility of each agency's Information Security Officer (ISO), or their designated backup, to notify the proper authorities of an incident by following these steps:

1. Agency notifies the CHP Emergency Notification and Tactical Alert Center (ENTAC) immediately upon discovery of the incident. Their 24-hour phone line is **(916) 657-8287**.
2. The State Information Security Office (SISO) and, in some cases, CHP's Computer Crimes Investigation Unit (CCIU) will contact the agency for additional details regarding the incident and to provide assistance as needed.
3. SISO provides agency with an incident number to be included on the Agency Security Incident Report (SIMM 65C).
4. Agency takes immediate steps to resolve the issue and, if necessary, makes notification to affected individuals.
5. Agency completes and submits the follow-up written report of incident (SIMM 65C) to the SISO within 10 business days from the date of the notification.
6. Agency implements corrective action steps identified in the report to rectify or mitigate the incident so it will not occur again.

State Information Security Office

Phone: (916) 445-5239

Email: security@dof.ca.gov

LEADING THE WAY TO SECURE THE
STATE'S INFORMATION ASSETS



INFORMATION SECURITY INCIDENT NOTIFICATION ROADMAP FOR STATE AGENCIES

FAQS FOR INFORMATION SECURITY INCIDENTS



**REPORT INCIDENTS
IMMEDIATELY!**

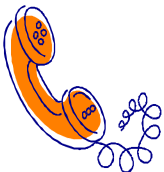
What is an information security incident?

An event that has reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset or information system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

What are some examples?

A complete list of reporting requirements is found in SAM Section 4845. However, the following are examples of a reportable incident:

- Theft, loss, damage, unauthorized destruction or modification of information, or unintentional or inappropriate release of confidential, sensitive or personal information (paper or electronic).
- Inappropriate use of an information asset or access by an employee or contractor which is not authorized or exceeds the limits of their authorized access.
- Loss or theft of any IT equipment, such as desktops, laptops, PDAs, or any electronic media which are capable of containing or storing confidential, sensitive, or personal information.
- Criminal activity, such as piracy, copyright infringement, and successful system or application hacks, exploited vulnerabilities, website defacements, virus attacks, and denial of service attacks. Service levels are usually, but not always, impacted by these types of events.
- Violations of agency security policy such as the downloading, storing or viewing inappropriate or illegal material on state systems.



Who should call the incident into ENTAC?

Typically the agency's Information Security Officer, or his/her backup, calls the incident into CHP.

What if I am not sure it is an incident or ENTAC does not take the report?

Contact the State Information Security Office (SISO) as soon as possible at **(916) 445-5239**.

What information should the person making the notification be prepared to give when calling CHP ENTAC?

Important things to be prepared to provide include:

- Reporting agency name
- Reporting person's contact information
- ISO and designated backup contact information
- Description of incident
- Date and time the incident occurred
- Date and time the incident was discovered
- Whether or not paper or electronic records were impacted?
- Whether or not the records contained personal, confidential, or sensitive (P/C/S) information?
- If known, how many records and individual's were impacted?
- If personal information was involved, whether or not the agency has or will be notifying the affected individuals?
- When applicable the make/model and IP address of the affected system, computer, electronic device, or media.
- Whether or not the electronic device or media, or P/C/S information on the device or media was encrypted and password protected.



What are the agency's responsibilities if the incident involves the theft or loss of personal information?

Besides reporting the incident to CHP and the SISO, the agency may be required by law to notify the affected individuals that there personal information has been lost or stolen. The Information Practices Act (Civil Code 1798 et .seq) defines a notice triggering event. Although, there is oftentimes good reason to notify the affected individuals even if it is not required by law.

What resources are available to an agency for assistance in handling an incident involving personal information?

The COPP and the SISO can provide assistance in handling any type of information security incident. See the other side of this brochure for contact information.

What is an incident response plan?

This is an internal agency plan which identifies what actions its employees must follow when an incident occurs to comply with statewide incident reporting requirements. It contains important contact information and procedures that should be followed for properly handling various types of incidents. Agencies should develop, implement, and make all employees aware of this plan BEFORE an incident occurs.

What resources are available to aid an agency in developing an incident response plan?

Information regarding the development an incident response plan is available on the SISO's Web site at www.infosecurity.ca.gov/incidents/ under "Other Resources".

Who else should the incident be reported to?

Depending upon the internal agency plan, its severity or if it has the capacity of a high profile incident, the agency may want to notify its cabinet-level management, its public information officer, and for HIPAA-impacted agencies, CalOHI must be notified.

Now that the incident has been reported to ENTAC, what are the agency's responsibilities?

First and foremost, the agency must take steps to resolve the issue.

Then an Agency Security Incident Report (SIMM 65C) must be completed, signed by the director, and submitted to the SISO within 10 business days of the incident being reported.

The corrective action plan identified in the report must be taken to mitigate further risk of occurrence.

Where do I find the Agency Incident Report (SIMM 65C)? The SIMM 65C is located on the SISO's Web site at www.infosecurity.ca.gov/tools/

My question was not addressed in this FAQ, is there more information?

Yes, more FAQs can be found on the SISO's Web site at www.infosecurity.ca.gov/Library/FAQs/

